

AO106 (Rev. 12/03) Affidavit for Search Warrant

**FILED**

## UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

FEB 28 2006

MAGISTRATE JUDGE  
DISTRICT OF NEVADA

DEPU

In the Matter of the Search of  
(Name, address or brief description of person, property or premises to be searched)

12720 Buckthorn Lane, Reno, Nevada

APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT

Case Number: 3:06-MJ-0023-VPC

I, MICHAEL WEST being duly sworn depose and say:I am a(n) SPECIAL AGENT, FEDERAL BUREAU OF INVESTIGATION and have reason to believe  
Official Titlethat ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

12720 Buckthorn Lane, Reno, Nevada, further described in Attachment A, fully incorporated by reference and attached hereto

in the \_\_\_\_\_ District of NEVADA

there is now concealed a certain person or property, namely (describe the person or property to be seized)

SEE ATTACHMENT B

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

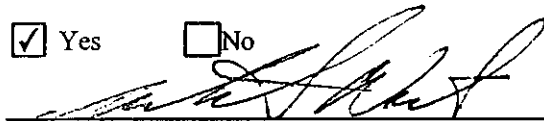
property that constitutes evidence of the commission of a criminal offense; the fruits of a crime, and/or property designed or intended for use which is or has been used as a means of committing a criminal offense

concerning a violation of Title 18 United States code, Section(s) 793(e)

The facts to support a finding of probable cause are as follows:

SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT MICHAEL WEST

Continued on the attached sheet and made a part hereof:

☒ Yes ☐ No
  
Signature of Affiant

Sworn to before me and subscribed in my presence,

February 28, 2006  
Date

at

RENO

NEVADA

City

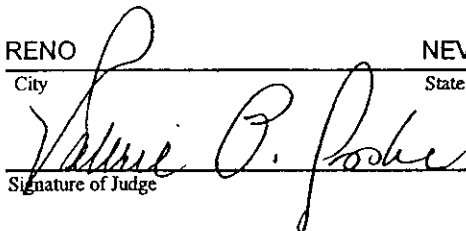
State

VALERIE P. COOKE

US MAGISTRATE

Name of Judge

Title of Judge

  
Signature of Judge

AFFIDAVIT

I, Michael A. West, Special Agent (SA), United States Federal Bureau of Investigation, being duly sworn, state the following:

I have been employed as a Special Agent with the Federal Bureau of Investigation for approximately ten years. As part of my regularly assigned duties, I investigate violations of federal statutes to include theft of trade secrets and the unlawful retention of information relating to the national defense which occur in Northern Nevada.

Your affiant makes this affidavit in support of the accompanying application for a search warrant for the premises located at 12720 Buckthorn Lane, Reno, Nevada (further described in "Attachment A").

Your affiant has investigated or been advised by other Special Agents of the U.S. Government and confirmed the following:

Your affiant became involved in investigating DENNIS LEE MONTGOMERY based on a complaint made by Management Committee Chairman Warren Trepp of eTreppid Technologies, LLC, a Nevada Limited Liability Corporation, located at 755 Trademark Drive, Reno, Nevada. Trepp alleged that Chief Technical Officer (CTO) DENNIS LEE MONTGOMERY removed eTreppid computer equipment and storage media containing Source Code files derived from eTreppid's development efforts relating to data compression and pattern recognition software, removed hard disk drives containing Secret information provided by the Department of Defense (DOD), and systematically deleted all Source Code files from the remaining eTreppid data servers, all in violation of Title 18, United States Code, Section 1832, Theft of Trade Secrets, and Title 18, United States Code, Section 793(e), Unlawful Retention of National Defense Information.

eTreppid Technologies, LLC, (eTreppid), a Nevada Limited Liability Company, was originally formed in 1998 as "Intrepid" by founders Warren Trepp (Trepp) and DENNIS LEE MONTGOMERY (MONTGOMERY) to develop software that relates to data compression and pattern recognition, among other products. Since that time and to the present, Trepp has held the

1 position of Management Committee Chairman and MONTGOMERY held the title of Chief  
2 Technical Officer (CTO).

3 MONTGOMERY signed a Contribution Agreement, dated September 28, 1998,  
4 in which MONTGOMERY effectively assigned all rights to his "Contributed Assets" to eTreppid  
5 in exchange for a fifty percent (50%) interest Management Interest in eTreppid. The "Contributed  
6 Assets" meant all of MONTGOMERY's know-how; trade secrets; patent rights, copyrights,  
7 trademarks, licenses and permits, registered or unregistered, pending or approved; software  
8 programs and all programming and Source Codes used in connection therewith or otherwise  
9 required to operate any component thereof; and all programming documentation, designs,  
10 materials and other information, all in whatever form and wherever located, relating to or used in  
11 connection with, or otherwise describing or consisting of any part of, the software compression  
12 technology.

13 MONTGOMERY also signed the "Amended And Restated Operating Agreement  
14 of eTreppid Technologies, LLC, A Nevada Limited Liability Company, Dated and Adopted  
15 Effective As Of November 1, 2002", which in paragraph 6.5, "Time Devoted to Management",  
16 MONTGOMERY agreed to "devote substantially all of his full time and attention and efforts to  
17 the Business and affairs of the LLC"; in paragraph 6.6, "Restriction on Independent Activities;  
18 Agreement Not to Compete", MONTGOMERY agreed that he "and his Affiliates, during the term  
19 of this Agreement, none of them shall compete with the LLC, whether for their own account  
20 and/or for the account of others, individually, jointly with others, or as a part of any other limited  
21 liability company, limited partnership, general partnership, joint venture, corporation or other  
22 entity, by: (i) developing, licensing, or exploiting in any manner any software programs or other  
23 technology which is competitive with the Technology or the Business of the LLC, or providing any  
24 services or supplies which are encompassed within the definition of the "Business" of the LLC set  
25 forth in this Agreement."  
26

1 MONTGOMERY, as the Chief Technical Officer, was responsible for leading the  
2 software development efforts of eTreppid, including those related to data compression, pattern  
3 recognition, change and anomaly detection, and other inventions, from 1998 until he was  
4 terminated on January 18, 2006.

5 MONTGOMERY filed ten Patent Assignment applications with the United States  
6 Patent and Trademark Office during the period of November 2000 to November 2001 for patents  
7 pertaining to various technologies developed by MONTGOMERY while an employee at eTreppid  
8 and on each patent MONTGOMERY assigned full and exclusive rights, title, and interest of these  
9 technologies to eTreppid.

10 Trepp considers eTreppid's trade secrets to be various software programs relating  
11 to data compression, pattern recognition, change and anomaly detection, among other things,  
12 which derive independent economic value, actual or potential, from not being generally known to,  
13 and not being readily ascertainable through proper means by the public. eTreppid has earned in  
14 excess of ten million dollars in revenues since 1998 from various government and commercial  
15 contracts. Trepp anticipates that eTreppid's development efforts will result in other multi-million  
16 dollar contracts.

17 eTreppid has taken reasonable steps to keep its information and development  
18 efforts secret by requiring Programmers or Software Developers to use unique user names and  
19 passwords to log onto eTreppid computers with limited access to prevent unauthorized  
20 duplication, modification, or deletion of Source Codes. Software Developers store their work or  
21 Source Code on a hard drive installed in their workstation and on a Source Code Server, a high  
22 capacity data storage device, which uses Redundant Array of Inexpensive Disks (RAID) storage to  
23 maintain and ensure reliable accessibility to the Source Code files produced by all Software  
24 Developers. The Source Code Server is backed up by the Internet Security Accelerator (ISA)  
25 Server which also uses RAID storage to maintain and ensure reliable accessibility to the Source  
26 Code files. Only two eTreppid employees, MONTGOMERY and Director of Research and

1 Development Sloan Venables, had the access rights to duplicate, modify, or delete Source Code  
2 files maintained on the Source Code and ISA Servers.

3 MONTGOMERY was responsible for and regularly maintained a separate backup  
4 copy of the Source Code Server data on an eTreppid black Lianli Central Processing Unit (CPU)  
5 connected to an Ultra Storage eight hard drive RAID storage unit, Model 2081, serial number  
6 6564737, located in a work area occupied by MONTGOMERY in the eTreppid warehouse.

7 As an additional security measure, Trepp required MONTGOMERY to provide  
8 him with periodic copies of eTreppid's current Source Code files on compact disks or hard drives  
9 over the past seven years which Trepp stored in a secure off-site location.

10 eTreppid's facility is physically secured by door locks, access control devices, and  
11 a monitored alarm system. eTreppid also maintains a video surveillance system that records  
12 sixteen surveillance cameras covering internal and external views of eTreppid's facility.

13 On March 12, 2003, eTreppid was awarded a contract from the U.S. Special  
14 Operations Command (SOCOM), Fort Bragg, North Carolina, to develop Automatic Target  
15 Recognition software which required eTreppid to have access to [REDACTED] material at other contractor  
16 and government locations. On August 1, 2005, SOCOM amended the Department of Defense  
17 (DOD) contract Security Classification Specification, DD Form 254, permitting eTreppid to store  
18 Secret material at the facility.

19 On or about August 25, 2003, MONTGOMERY received and signed a Security  
20 Briefing from Michael S. Allen, Department of the Army, U.S. Army Security Operations Training  
21 Facility (SOTF), Fort Bragg, North Carolina, regarding MONTGOMERY's obligation to protect  
22 either sensitive or classified material which concern the security of the United States of America  
23 due to MONTGOMERY's assignment, employment, or association with SOTF.

24 On or about September 16, 2003, MONTGOMERY received another Security  
25 Briefing from the Defense Security Service, Nellis Air Force Base (AFB), Las Vegas, Nevada, and  
26 signed a Standard Form 312, "Classified Information Nondisclosure Agreement", in which

1 MONTGOMERY was made aware of his obligation to protect from unauthorized disclosure,  
2 unauthorized retention, or negligent handling of classified information, marked or unmarked,  
3 which could cause damage or irreparable injury the United States or could be used to advantage by  
4 a foreign nation.

5 During the period of November 9, 2005 to November 18, 2005 [REDACTED]  
6 [REDACTED], traveled to [REDACTED] located on the  
7 Nellis AFB, and recorded [REDACTED] video images onto nine eTreppid hard drives for  
8 use in the development of the Automatic Target Recognition software. [REDACTED] marked the nine hard  
9 drives with red standard U.S. Government [REDACTED] labels as instructed by contractor personnel at  
10 Nellis AFB and placed a hand written descriptor label on each of the nine hard drives. [REDACTED]  
11 subsequently mailed the nine [REDACTED] hard drives to eTreppid in Reno, Nevada, and these [REDACTED]  
12 hard drives were stored in a GSA approved safe as required by the DOD. [REDACTED] Trepp, and  
13 MONTGOMERY were the only eTreppid employees with the combination to the safe.

14 On or about December 6, 2005, [REDACTED] discovered that the nine [REDACTED] hard drives  
15 were not in the GSA approved safe and notified Trepp who told MONTGOMERY to store the  
16 [REDACTED] hard drives correctly in the GSA approved safe. On or about December 7, 2005,  
17 MONTGOMERY told [REDACTED] all the [REDACTED] hard drives were stored in a file cabinet in the  
18 warehouse. [REDACTED] informed MONTGOMERY that this was not the correct location to store the  
19 [REDACTED] hard drives and notified Trepp. On December 8, 2005, all nine [REDACTED] hard drives were  
20 returned to a GSA approved safe which was accessible by [REDACTED], Trepp, and MONTGOMERY.

21 On or about December 13, 2005, [REDACTED] was completing work on copying selected  
22 data from the [REDACTED] hard drives to four Mini DV cassette tapes at the request of Trepp. [REDACTED]  
23 found the nine [REDACTED] hard drives missing from the GSA approved safe and notified Trepp.  
24 MONTGOMERY returned all nine [REDACTED] hard drives to the GSA approved safe. Later on  
25 December 13, 2005, [REDACTED] handed MONTGOMERY two Mini DV cassette tapes labeled [REDACTED].  
26 [REDACTED] placed the two other [REDACTED] Mini DV cassette tapes in the top drawer of the GSA approved

1 safe and changed the combination so she was the only one with the combination.

2 MONTGOMERY told [REDACTED] he was condensing the nine original [REDACTED] hard drives as some were  
3 only partially full. MONTGOMERY eventually provided [REDACTED] with the nine original [REDACTED] hard  
4 drives and six additional hard drives labeled [REDACTED] by MONTGOMERY. Gray secured the nine  
5 original [REDACTED] hard drives and the six [REDACTED] hard drives containing copies of the nine original  
6 [REDACTED] hard drives in the bottom drawer of the GSA approved safe. The bottom drawer of the  
7 GSA approved safe was only accessible by [REDACTED] Trepp, and MONTGOMERY.

8 On or about December 15, 2005, [REDACTED] again found all nine original [REDACTED] hard  
9 drives missing from the GSA approved safe. MONTGOMERY told [REDACTED] that he wanted to store  
10 the hard drives in the file cabinet in the warehouse. [REDACTED] informed MONTGOMERY this was not  
11 the appropriate way to secure classified content and he was risking losing his security clearance.  
12 MONTGOMERY stated "I don't care about my clearance. They'll always give me my clearance  
13 because they want me to do the work". [REDACTED] notified Trepp and Trepp agreed that access to the  
14 classified material needed to be restricted and instructed [REDACTED] to place all classified material in the  
15 top drawer of the GSA approved safe. [REDACTED] changed the combination to the top drawer and was  
16 the only eTreppid employee with the combination. [REDACTED] secured all classified material in the top  
17 drawer of the GSA approved safe, to include the nine original [REDACTED] hard drives.

18 On or about Sunday, December 18, 2005, MONTGOMERY attempted to contact  
19 [REDACTED] by text message to get access to the classified material. Eventually, Trepp contacted [REDACTED] by  
20 telephone and instructed [REDACTED] to give MONTGOMERY the combination to the top drawer of the  
21 GSA approved safe so MONTGOMERY could work and all classified material would be re-  
22 secured on Monday.

23 On or about December 19, 2005 or December 20, 2005, [REDACTED] a Software  
24 Developer at eTreppid, observed MONTGOMERY delete eTreppid Source Code files from the  
25 hard drive installed in [REDACTED] computer workstation which [REDACTED] had not recently used.  
26 MONTGOMERY stated he deleted the files for security reasons and copies of these files were



1 accessible on the Source Code Server. At that time, [REDACTED] observed that more recent Source Code  
2 files [REDACTED] used in [REDACTED] development efforts remained on [REDACTED] hard drive installed in [REDACTED] computer  
3 workstation.

4 On or about December 21, 2005, [REDACTED] and  
5 [REDACTED] discovered that the Central Processing Unit and RAID storage unit used by  
6 MONTGOMERY to backup the Source Code Server was missing. [REDACTED] asked  
7 MONTGOMERY what happened to the Central Processing Unit and RAID storage unit and  
8 MONTGOMERY stated he took them home. [REDACTED] described the missing equipment as a  
9 black Lianli Central Processing Unit (CPU) connected to an Ultra Storage eight hard drive RAID  
10 storage unit, Model 2081, serial number 6564737. [REDACTED] stated this equipment is large and  
11 heavy. [REDACTED] has never known MONTGOMERY to remove this equipment from the eTreppid  
12 facility as MONTGOMERY used the equipment on a daily basis.

13 Also on December 21, 2005, [REDACTED] installed and activated the Internet Security  
14 Accelerator (ISA) Server designed to back up all of eTreppid's server's data, including the Source  
15 Code Server. Prior to leaving eTreppid on December 21, 2005, [REDACTED] verified that the ISA  
16 Server was operating properly and noted data was being successfully completed from eTreppid  
17 servers.

18 On or about December 22, 2005, [REDACTED] departed Reno, Nevada,  
19 for the Christmas holiday and did not return to Reno, Nevada, until January 3, 2006.

20 In December 2005, right before the Christmas holiday, [REDACTED] a  
21 Software Developer at eTreppid, noticed the collection of eTreppid Source Code files that [REDACTED] had  
22 stored on the hard drive installed in [REDACTED] computer workstation had been deleted. [REDACTED] asked  
23 MONTGOMERY about these files and MONTGOMERY explained that he was backing up  
24 eTreppid Source Code and would provide [REDACTED] the portion eTreppid Source Code necessary for  
25 [REDACTED] to work. Between December 25, 2005, and January 1, 2006, [REDACTED] would request eTreppid  
26 Source Code file from MONTGOMERY and MONTGOMERY would place the request Source



1 Code file on a shared drive where [REDACTED] retrieved the Source Code file. Upon completing his  
2 work on that Source Code file, [REDACTED] would copy the file back to the shared drive and inform  
3 MONTGOMERY who was responsible for copying that file to the Source Code Server.

4 On or about December 23, 2005, [REDACTED], an employee at eTreppid, moved  
5 six closed boxes from MONTGOMERY's office to the back door of the warehouse at  
6 MONTGOMERY's request. [REDACTED] was not aware of the contents of these boxes. [REDACTED]  
7 observed MONTGOMERY load at least two of these boxes into MONTGOMERY's truck.  
8 [REDACTED] has never known MONTGOMERY to remove anything from the facility in the past.

9 On or about January 3, 2006, [REDACTED] returned from vacation and noticed the  
10 Source Code Server cabinet and keyboard were in disarray. [REDACTED] entered the Server Room  
11 and found the Source Code Server screen active and could see a process running on the screen.  
12 Shortly thereafter, MONTGOMERY entered the Server Room and [REDACTED] asked  
13 MONTGOMERY what he was doing. MONTGOMERY stated he was "cleaning stuff up."  
14 [REDACTED] went to the warehouse to further discuss what MONTGOMERY was doing on the  
15 Source Code Server and MONTGOMERY stated he was just "cleaning stuff up" and deleting old  
16 files. While in the warehouse, [REDACTED] noticed the Central Processing Unit and RAID storage  
17 unit used by MONTGOMERY to backup the Source Code Server was still missing. On or about  
18 January 3, 2006, [REDACTED] asked MONTGOMERY where was the equipment and  
19 MONTGOMERY stated "I'll bring it back, I don't need it anymore."

20 [REDACTED] looked at the Source Code Server and found that the majority of the  
21 Source Code files contained in specific folders used by the Software Developers had been  
22 systematically deleted. [REDACTED] attempted to access the ISA Server which [REDACTED] found inoperable  
23 and unable to access.

24 On or about January 9, 2005, Trepp became aware that the Source Code was  
25 missing when his employees complained that they were unable to operate their computer systems.  
26 Trepp asked [REDACTED] about the problem and was told by [REDACTED] that all eTreppid's Source

1 Code had been deleted from the Source Code Server, the ISA Server, and all of eTreppid's  
2 Software Developer's workstations. Trepp confronted MONTGOMERY who said that the Source  
3 Code could be located on the 753 removable hard drives located at the company. Trepp instructed  
4 eTreppid employees to conduct an analysis of each of the company's 753 hard drives in an effort  
5 to locate the Source Code. The two day analysis failed to locate the Source Code.

6 While looking for the Source Code on eTreppid hard drives, [REDACTED] located seven  
7 hard drives containing copies of the nine original [REDACTED] hard drives recorded at Nellis AFB in  
8 MONTGOMERY's file cabinet. [REDACTED] checked the drawer in the GSA approved safe where all  
9 [REDACTED] material was to be maintained and found seven more hard drives containing copies of the  
10 nine original [REDACTED] hard drives recorded at Nellis AFB. A complete search of the eTreppid  
11 facility failed to locate the nine original [REDACTED] hard drives recorded or two [REDACTED] Mini DV  
12 cassette tapes containing copied segments of the original [REDACTED] hard drives. [REDACTED] stated that [REDACTED]  
13 and MONTGOMERY were the only eTreppid employees with access to the top drawer of the  
14 GSA approved safe.

15 On or about January 10, 2006, Trepp instructed [REDACTED] to review eTreppid's  
16 video surveillance system. [REDACTED] found that each of the sixteen computer systems were no  
17 longer recording video from eTreppid's sixteen cameras. [REDACTED] also found that all video  
18 footage stored on the sixteen computer systems had been deleted.

19 MONTGOMERY returned to eTreppid on morning of January 10, 2006, when  
20 [REDACTED] asked MONTGOMERY where was eTreppid's Source Code. MONTGOMERY stated it  
21 was on 320 gigabyte hard drives in the building. No such hard drives were located.  
22 MONTGOMERY again returned to eTreppid later on January 10, 2006, and [REDACTED] again asked  
23 MONTGOMERY where a certain part of the Source Code to which MONTGOMERY stated "he  
24 (Trepp) needs to give me big money if he wants it."

25 Trepp retrieved the annual or periodic copies provided to him by  
26 MONTGOMERY over the last seven years from the secure off-site location. [REDACTED] conducted

1 a review of the compact disks and hard drives provided by MONTGOMERY and found that these  
2 compact disks and hard drives contained no data relevant to eTreppid's development efforts or  
3 Source Code except for one program developed in 2002 which is currently not being used.

4 Trepp advised the MONTGOMERY devoted eight years of his life to developing  
5 various software products at eTreppid, including to data compression, pattern recognition, change  
6 and anomaly detection. MONTGOMERY worked on these products every day during normal  
7 business hours and would often return at night and on weekends to continue his efforts.

8 MONTGOMERY considered some of these capabilities to be of paramount importance to him  
9 (MONTGOMERY) that he (MONTGOMERY) would never delegate the project to someone else.

10 Trepp further advised if MONTGOMERY intended to continue work on eTreppid's Source Code,  
11 MONTGOMERY would need substantial computing power, similar to the workstation and RAID  
12 unit removed from the warehouse, and access to video images contained on the nine Secret hard  
13 drives.

14 MONTGOMERY did not return to eTreppid after January 10, 2006, and has not  
15 returned any eTreppid property. MONTGOMERY was terminated as an employee of eTreppid on  
16 January 18, 2006.

17 [REDACTED]  
18 [REDACTED]  
19 [REDACTED]  
20 [REDACTED]  
21 [REDACTED]  
22 [REDACTED]  
23 [REDACTED]  
24 [REDACTED]  
25  
26

1 Based on the conversation MONTGOMERY had with [REDACTED] and possibly  
2 other unknown individuals, it appears that MONTGOMERY may have provided information  
3 relating to the Source Code to others and is looking for investors for the Source Code.

4 [REDACTED]  
5 [REDACTED]  
6 [REDACTED]  
7 [REDACTED]  
8 [REDACTED]  
9 [REDACTED]  
10 [REDACTED]  
11 [REDACTED]  
12 [REDACTED]  
13 [REDACTED]  
14 [REDACTED]  
15 [REDACTED]  
16 [REDACTED]  
17 [REDACTED]  
18 [REDACTED]  
19 [REDACTED]  
20 [REDACTED]  
21 [REDACTED]  
22 [REDACTED]  
23 [REDACTED]  
24 [REDACTED]  
25 [REDACTED]  
26 [REDACTED]

1

2

3

4

5

6

7

8

9

Instrumentalities and Evidence of the Crime

10

11

12

13

14

15

16

17

18

19

Seizure of Equipment and Data

20

21

22

23

24

25

26

As set forth above, there is probable cause to believe that the premises located at 12720 Buckthorn Lane, Reno, Nevada, contains evidence of the offense of Theft of Trade Secrets and Unlawful Retention of National Defense Information. Therefore, the computer hardware, software, computer documentation, passwords, and data security devices further described in Attachment B constitute means of committing criminal offenses. Additionally, there is probable cause to believe that MONTGOMERY has used his computers and related electronic storage devices to collect, store, maintain, retrieve, conceal, transmit, and use electronic data relating to these offenses in the form of electronic records, documents, and materials, including those used to facilitate communications, each of which constitutes evidence of the offense.

Based on my knowledge, training, and experience, and my conversations with other FBI Special Agents and computer trained personnel, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate

1 such a computer, be seized and subsequently processed by a certified Computer Forensic Examiner  
2 in a laboratory setting. This is true because of the following:

3 a. The volume of evidence. Computer storage devices (such as hard disks,  
4 DVDs, compact disks, diskettes, tapes, laser disks, and other storage devices.) can store the  
5 equivalent of thousands of pages of information. Additionally, a user may seek to conceal  
6 criminal evidence by storing it in random order with deceptive file names. Searching authorities  
7 are required to examine all the stored data to determine which particular files are evidence or  
8 instrumentalities of criminal activity. This sorting process can take weeks or months, depending  
9 on the volume of data stored, and it would be impractical to attempt this kind of data analysis on-  
10 site.

11 b. Technical requirements. Analyzing computer systems for criminal  
12 evidence is a highly technical process requiring expert skill and a properly controlled environment.  
13 The vast array of computer hardware and software available requires even computer experts to  
14 specialize in some systems and applications. Thus it is difficult to know prior to the search which  
15 expert possesses sufficient specialized skill to best analyze the system and its data. No matter  
16 which system is used, however, data analysis protocols are exacting scientific procedures, designed  
17 to protect the integrity of the evidence and to recover even "hidden", erased, compressed,  
18 password-protected, or encrypted files. Since computer evidence is extremely vulnerable to  
19 tampering or destruction (both from external sources or from destructive code imbedded in the  
20 system as a "booby trap"), a controlled environment is essential to its complete and accurate  
21 analysis.

22 Due to the volume of the data at issue and the technical requirements set forth  
23 above, it may be necessary that the above reference equipment, software, data, and related  
24 instruction be seized and subsequently processed by a certified Computer Forensic Examiner in a  
25 laboratory setting. Under appropriate circumstance, some types of computer equipment can be  
26 more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal

1 from the premises. One factor used in determining whether to analyze a computer on-site or to  
2 remove it from the premises is whether the computer constitutes an instrumentality of an offense  
3 and is thus subject to immediate seizure as such--or whether it serves as a mere repository for  
4 evidence of a criminal offense. Another determining factor is whether, as a repository for  
5 evidence, a particular device can be more readily, quickly, and thus less intrusively, analyzed off  
6 site, with due considerations given to preserving the integrity of the evidence. This, in turn, is  
7 often dependent upon the amount of data and number of discrete files or file areas that must be  
8 analyzed, and this is frequently dependent upon the particular type of computer hardware involved.  
9 As a result, it is ordinarily impossible to appropriately analyze such material without removing it  
10 from the location where it is seized.

#### 11 Analysis of Electronic Data

12 The analysis of electronically stored data, whether performed on-site or in a  
13 laboratory or other controlled environment, may entail any or all of several different techniques.  
14 Such techniques may include, but shall not be limited to, surveying various file "directories" and  
15 the individual files they contain (analogous to looking at the outside of a file cabinet for the  
16 markings it contains and opening a drawer capable of containing pertinent files, in order to locate  
17 the evidence and instrumentalities authorized for seizure by the warrant); "opening" or reading the  
18 first few "pages" of such files in order to determine their precise contents; "scanning" storage areas  
19 to discover and possibly recover recently deleted data; scanning storage areas for deliberately  
20 hidden files; and performing electronic "key-word" searches through all electronic storage areas to  
21 determine whether occurrences of language contained in such storage areas exist that are  
22 intimately related to the subject matter of the investigation.

23  
24 Based on the investigation [REDACTED] made to  
25 MONTGOMERY, MONTGOMERY appears to have removed the necessary computer equipment  
26 and data from eTreppid to continue his development efforts and more likely than not maintains



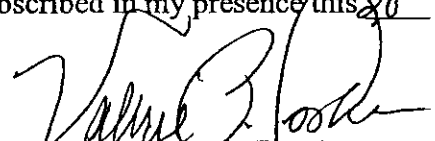
1 this computer equipment and data at his residence located at 12720 Buckthorn Lane, Reno,  
2 Nevada.

3 Based on the forgoing, your affiant believes there is reasonable grounds and  
4 probable cause to believe that DENNIS LEE MONTGOMERY did steal trade secrets, a violation  
5 of Title 18, United States Code, Section 1832, Theft of Trade Secrets, and unlawful retained  
6 National Defense Information, a violation of Title 18, United States Code, Section 793(e),  
7 Unlawful Retention of National Defense Information.

8 Wherefore, your affiant requests a search warrant for the premises located at 12720  
9 Buckthorn Lane, Reno, Nevada (further described in "Attachment A") for the purpose of locating  
10 and seizing items listed in Attachment B.

11  
12   
13 MICHAEL A. WEST, Special Agent  
Federal Bureau of Investigation

14 Sworn to before me and subscribed in my presence this 28<sup>th</sup> day of February 2006.

15  
16   
17 VALERIE P. COOKE  
18 United States Magistrate Judge  
19  
20  
21  
22  
23  
24  
25  
26

ATTACHMENT A

12720 Buckthorn Lane, Reno, Nevada, is a single family residence located on the westside of Buckthorn Lane. The residence is a single level home having an off-white stucco exterior and an attached three car garage with white garage doors facing Buckthorn Lane. The numbers "12720" are affixed to the southern corner of the garage structure and two planters with small green trees are located on either side of the entryway arch.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Any Black Lianli Central Processing Unit (CPU)
2. Any Ultra Storage eight hard drive RAID storage unit, Model 2081, serial number 6564737.
3. Any address and/or telephone books and papers reflecting names, addresses, telephone numbers, electronic mail addresses, and/or Internet Web site addresses which might identify associates which may relate to potential investors of the Source Code.
4. Any telephone bills and records, and/or calling cards numbers which may relate to potential investors of the Source Code.
5. Any corporate documents, corporate charters, articles of incorporation, list of corporate officers, and/or registered agent applications which may relate to potential investors of the Source Code.
6. Any bank statements, deposit or withdrawal slips, bank checks, money orders, cashier's checks, passbooks, wire transfers, and any other items evidencing the movement of money which may relate to payments made and/or received from potential investors of the Source Code.
7. Any personal or business correspondence, both written forms and electronically stored, to include envelopes and packaging materials which indicate indica of occupancy.
8. Any computer files protected by copyright, including software and movie files, log files, user names and passwords to Internet, mIRC, ftp, or other sites, programs or software used for communication between individuals relating to Dennis Lee Montgomery and other unknown individuals.
9. Any computer hardware, meaning any and all computer equipment including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
10. Any computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the

1 operation of computer software, such as operating systems software, applications  
2 software, utility programs, compilers, interpreters, communications software, and other  
programming used or intended to be used to communicate with computer components.

3 11. Any computer-related documentation, meaning any written, recorded, printed, or  
4 electronically-stored material which explains or illustrates the configuration or use of any  
seized computer hardware, software, or related items.

5 12. Any computer passwords and data security devices, meaning any devices, programs, or  
6 data -- whether themselves in the nature of hardware or software -- that can be used or are  
7 designed to be used to restrict access to, or to facilitate concealment of, any computer  
8 hardware, computer software, computer-related documentation, or electronic data records.  
9 Such items include, but are not limited to, data security hardware (such as encryption  
devices, chips, and circuit boards); passwords; data security software or information (such  
as test keys and encryption codes); and similar information that is required to access  
computer programs or data or to otherwise render programs or data into usable form.

10 13. Any computer or electronic records, documents, and materials, including those used to  
11 facilitate interstate communications, in whatever form and by whatever means such  
12 records, documents, or materials, their drafts or their modifications, may have been  
13 created or stored, including, but not limited to, any hand-made form (such as writing or  
14 marking with any implement on any surface, directly or indirectly); any photographic  
15 form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures  
or photocopies); any mechanical form (such as photographic records, printing or typing);  
any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact  
disks); or any information on an electronic or magnetic storage device (such as floppy  
diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory  
calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts  
from any magnetic storage device.

16 14. Any electronic information or data, stored in any form, which has been used or prepared  
17 for use either for periodic or random backup (whether deliberate, inadvertent, or  
18 automatically or manually initiated), of any computer or computer system. The form such  
19 information might take includes, but is not limited to, floppy diskettes, fixed hard disks,  
removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and  
other media capable of storing magnetic or optical coding.

20 15. Any electronic storage device capable of collecting, storing, maintaining, retrieving,  
21 concealing, transmitting, and using electronic data, in the form of electronic records,  
22 documents, and materials, including those used to facilitate interstate communications.  
23 Included within this paragraph is any information stored in the form of electronic,  
magnetic, optical, or other coding on computer media or on media capable of being read  
24 by a computer or computer-related equipment, such as fixed disks, external hard disks,  
25 removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes,  
26 optical storage devices, laser disks, or other memory storage devices.